UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/448,154	11/24/1999	PAUL S. GERMSCHEID	33012/274/10	4721

27516 7590 05/04/2005

UNISYS CORPORATION
MS 4773
PO BOX 64942
ST. PAUL, MN 55164-0942

EXAMINER	
WASSUM, LUKE S	

ART UNIT	PAPER NUMBER
2167	

DATE MAILED: 05/04/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/448,154	GERMSCHEID ET AL.	
	Examiner	Art Unit	
	Luke S. Wassum	2167	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 December 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *25 April 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 30 December 2004 has been entered.

Response to Preliminary Amendment

2. The Applicants' preliminary amendment, filed 30 December 2004, has been received, entered into the record, and considered.

3. As a result of the amendment, claims 1, 2, 11 and 16 have been amended. Claims 1-20 remain pending in the application.

The Invention

4. The claimed invention is an apparatus for and method of using an Internet terminal coupled to the World Wide Web to access an existing proprietary database management system, wherein said accessing does not require the transmission of a user identifier across the Internet, thereby enhancing security. Sign in information from a user (such as a user id and password) is processed only at the Internet terminal, and only a special field indicative of the site specific user validation data is transmitted over the Internet as part of the service request.

Specification

5. Applicant has incorporated by reference numerous co-pending applications at various points in the specification. Examiner notes that incorporation by reference of an application in a printed United States Patent constitutes a special circumstance under 35 U.S.C. § 122 warranting that access of the original disclosure of the application be granted. The incorporation by reference will be interpreted as a waiver of confidentiality of only the original disclosure as filed, and not the entire application file. See *In re Gallo*, 231 USPQ 496 (Comm'r Pat. 1986).

If Applicant objects to access to the entire application file(s), two copies of the information incorporated by reference must be submitted along with the objection. Failure to provide the material within the period provided will result in the entire application(s) (including prosecution) being made available to petitioner. The Office will not attempt to separate the noted materials from the remainder of the application. See *In re Marsh Engineering Co*, 1913 C.D. 183 (Comm'r Pat. 1913).

Claim Rejections - 35 USC § 112

6. In view of the Applicants' arguments regarding the rejection of claims 1-20 under 35 U.S.C. § 112, first paragraph, the examiner withdraws these rejections.

7. In view of the amendments to claims 1 and 2, the examiner withdraws the pending rejection of these claims under 35 U.S.C. § 112, second paragraph.

8. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

9. Claims 3-5, 8-10, 12-15 and 18-20 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

10. Regarding claims 3, 8, 12 and 18, the claim language is inconsistent with the disclosure of the invention. This inconsistency renders the claims indefinite, in accordance with MPEP § 2173.03[R-1]:

> "Although the terms of a claim may appear to be definite, inconsistency with the specification disclosure or prior art teachings may make an otherwise definite claim take on an unreasonable degree of uncertainty. In re Cohn, 438 F.2d 989, 169 USPQ 95 (CCPA 1971); In re Hammack, 427 F.2d 1378, 166 USPQ 204 (CCPA 1970). In Cohn, the claim was directed to a process of treating a surface with a corroding solution until the metallic appearance is supplanted by an "opaque" appearance. Noting that no claim may be read apart from and independent of the supporting disclosure on which it is based, the court found that the description, definitions and examples set forth in the specification relating to the appearance of the surface after treatment were inherently inconsistent and rendered the claim indefinite."

In this case, the Summary of the Invention, the Abstract, and the claims all state that the 'special field' (Abstract)/user[site] identifier (claims 3, 8, 12 and 18)/information (page 7, lines 17-18) is transmitted as part of the service request, but this conflicts with the specification regarding Figure 10.

On page 33, second paragraph, the specification discloses that a service request is transferred to web server 314 via world wide web path 306, and then passed to Cool ICE Service Handler 332 for retrieval of the command language script which describes the activities required of the database management system to respond to the service request. Next, the command language script and any

associated security profile is transferred from repository 342 to the Cool ICE Service Handler 332 for execution.

On page 34, last paragraph, it is disclosed that if a security profile is associated with the service request, the Cool ICE Service Handler 332 sends a request back to the user to provide a user-id. In other words, the service request is received, the corresponding script (and security profile) is retrieved, and only then is a request made for the transmission of the user/site identifier.

This disclosure conflicts with claims 3, 8, 12 and 18, which contain the limitation that the user/site identifier is transmitted to the web server as part of the service request. This conflict renders claims 3, 8, 12 and 18 indefinite.

11. Claims 4, 5, 9, 10, 13-15, 19 and 20, fully incorporating the deficiencies of their respective parent claims, are likewise rejected.

Claim Rejections - 35 USC § 103

12. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

13. The factual inquiries set forth in *Graham* v. *John Deere Co*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

14. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

15. Claims 1-4, 6-8, 11-14 and 16-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Garrison** (U.S. Patent 6,275,939) in view of **De Capitani di Vimercati et al.** ("Access Control in Federated Systems") in view of **Steele et al.** (U.S. Patent 6,282,175).

16. Regarding claim 1, **Garrison** teaches a data processing environment having a user with a user identifier which uniquely identifies said user at a terminal at a particular site which generates a service request requesting access to secure data responsively coupled via a publicly accessible digital data communication network to a database management system having at least one database containing said secure data as claimed, comprising a security profile whereby said database management system permits said terminal to access said at least one database (see col. 4, lines 1-32; see also col. 6, line 60 through col. 7, line 32; see also col. 7, line 50 through col. 8, line 37), wherein

the existence of the security profile renders the claimed administration module inherent, since the only claimed functionality if the administration module is to maintain the security profile, and the reference teaches the maintenance of a security profile at col. 7, lines 50-67 and col. 10, lines 5-17.

Garrison does not explicitly teach a data processing environment wherein the user accesses the database by transferring a second user identifier which uniquely identifies a particular site without transfer of said user identifier via said publicly accessible digital data communication network.

De Capitani di Vimercati et al., however, teaches a data processing environment wherein the user accesses the database by transferring a second user identifier which uniquely identifies a particular site without transfer of said user identifier via said publicly accessible digital data communication network (see page 88, col. 2, last paragraph; see also Table 1; see also section 3.2 Authentication, beginning on page 94, all of which teach a mechanism whereby all users accessing a database from a particular site are granted access).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the references, since they are all concerned with the same field of endeavor, that is, remotely accessing databases (see **Garrison**, Abstract; see also **De Capitani di Vimercati et al.**, Abstract).

It would have been furthermore obvious to one of ordinary skill in the art at the time of the invention to provide an authentication mechanism whereby the user identifier need not be transmitted via a publicly accessible digital communication network (i.e., global authentication), since

the alternative would be to impose local authentication, wherein users are required to re-authenticate themselves at each local site, which may make the access control process very heavy (see **De Capitani di Vimercati et al.**, page 87, col. 2, last paragraph through page 88, col. 1, first paragraph).

Neither **Garrison** nor **De Capitani di Vimercati et al.** explicitly teaches a data processing environment wherein said service request is honored by executing a sequence of command language scripts having an associated security profile.

Steele et al., however, teaches a data processing environment wherein a service request is honored by executing a sequence of command language scripts having an associated security profile (see col. 4, line 57 through col. 5, line 4; see also col. 7, lines 33-56).

It would have been obvious to one of ordinary skill in the art at the time of the invention to satisfy service requests through the execution of command language scripts having an associated security profile, since upon receipt of the service request the request can be satisfied merely by executing the corresponding predefined command language script (see **Steele et al.**, col. 7, lines 33-56), without the necessity to first translate the request into a valid SQL command and then submit the SQL command to the database (as is the case in **Garrison**, col. 8, lines 9-19).

17. Regarding claim 6, **Garrison** teaches an apparatus as claimed, comprising:

a) a terminal located at a particular location (see col. 4, lines 1-32) having a user with a user identifier which identifies said user (see col. 6, line 60 through col. 7, line 13);

b) a database management system having access to a database responsively coupled to said user terminal via a publicly accessible digital data communication network (see col. 4, lines 1-32); and

c) a security profile generated by said database management system whereby said database management system provides access to a particular secure portion of said database corresponding to said security profile (see col. 7, line 50 through col. 8, line 37).

Garrison does not explicitly teach an apparatus wherein the user accesses the database by transferring a second user identifier which uniquely identifies a particular site without transfer of said user identifier via said publicly accessible digital data communication network.

De Capitani di Vimercati et al., however, teaches an apparatus wherein the user accesses the database by transferring a second user identifier which uniquely identifies a particular site without transfer of said user identifier via said publicly accessible digital data communication network (see page 88, col. 2, last paragraph; see also Table 1; see also section 3.2 Authentication, beginning on page 94, all of which teach a mechanism whereby all users accessing a database from a particular site are granted access).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the references, since they are all concerned with the same field of endeavor, that is, remotely accessing databases (see **Garrison**, Abstract; see also **De Capitani di Vimercati et al.**, Abstract).

It would have been furthermore obvious to one of ordinary skill in the art at the time of the invention to provide an authentication mechanism whereby the user identifier need not be transmitted via a publicly accessible digital communication network (i.e., global authentication), since the alternative would be to impose local authentication, wherein users are required to re-authenticate themselves at each local site, which may make the access control process very heavy (see **De Capitani di Vimercati et al.**, page 87, col. 2, last paragraph through page 88, col. 1, first paragraph).

Neither **Garrison** nor **De Capitani di Vimercati et al.** explicitly teaches an apparatus wherein said service request is honored by executing a sequence of command language scripts having an associated security profile.

Steele et al., however, teaches an apparatus wherein a service request is honored by executing a sequence of command language scripts having an associated security profile (see col. 4, line 57 through col. 5, line 4; see also col. 7, lines 33-56).

It would have been obvious to one of ordinary skill in the art at the time of the invention to satisfy service requests through the execution of command language scripts having an associated security profile, since upon receipt of the service request the request can be satisfied merely by executing the corresponding predefined command language script (see **Steele et al.**, col. 7, lines 33-56), without the necessity to first translate the request into a valid SQL command and then submit the SQL command to the database (as is the case in **Garrison**, col. 8, lines 9-19).

18. Regarding claim 11, **Garrison** teaches a method of utilizing a user terminal having a user with a user identifier located at a site to securely access a remote database management system having a database via a publicly accessible digital data communication network as claimed, comprising:

a) signing on to said terminal by said user utilizing said user identifier (see col. 2, line 64 through col. 3, line 2, disclosing that the client transmits a password to the client to identify the user of the client system, meaning that the user has necessarily signed on to the client system utilizing a user identifier);

b) transmitting a service request requiring secure access to said database from said terminal (see col. 6, line 60 through col. 7, line 32; see also col. 7, line 50 through col. 8, line 37);

c) receiving said service request by said remote database management system (see col. 6, line 60 through col. 7, line 32; see also col. 7, line 50 through col. 8, line 37);

d) determining a security profile (see col. 6, line 60 through col. 7, line 32; see also col. 7, line 50 through col. 8, line 37), wherein the existence of the security profile renders the claimed administration module inherent, since the only claimed functionality if the administration module is to maintain the security profile, and the reference teaches the maintenance of a security profile at col. 7, lines 50-67 and col. 10, lines 5-17;

e) comparing said security profile with said service request (see col. 6, line 60 through col. 7, line 32; see also col. 7, line 50 through col. 8, line 37); and

f) honoring said service request if and only if said service request corresponds to said security profile (see col. 6, line 60 through col. 7, line 32; see also col. 7, line 50 through col. 8, line 37).

Garrison does not explicitly teach a method wherein the user accesses the database without transfer of said user identifier via said publicly accessible digital data communication network.

De Capitani di Vimercati et al., however, teaches a method wherein the user accesses the database without transfer of said user identifier via said publicly accessible digital data communication network (see page 88, col. 2, last paragraph; see also Table 1; see also section 3.2 Authentication, beginning on page 94, all of which teach a mechanism whereby all users accessing a database from a particular site are granted access).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the references, since they are all concerned with the same field of endeavor, that is, remotely accessing databases (see **Garrison**, Abstract; see also **De Capitani di Vimercati et al.**, Abstract).

It would have been furthermore obvious to one of ordinary skill in the art at the time of the invention to provide an authentication mechanism whereby the user identifier need not be transmitted via a publicly accessible digital communication network (i.e., global authentication), since the alternative would be to impose local authentication, wherein users are required to re-authenticate themselves at each local site, which may make the access control process very heavy (see **De Capitani di Vimercati et al.**, page 87, col. 2, last paragraph through page 88, col. 1, first paragraph).

Neither **Garrison** nor **De Capitani di Vimercati et al.** explicitly teaches a method wherein said service request is honored by executing a sequence of command language scripts having an associated security profile.

Steele et al., however, teaches a method wherein a service request is honored by executing a sequence of command language scripts having an associated security profile (see col. 4, line 57 through col. 5, line 4; see also col. 7, lines 33-56).

It would have been obvious to one of ordinary skill in the art at the time of the invention to satisfy service requests through the execution of command language scripts having an associated security profile, since upon receipt of the service request the request can be satisfied merely by executing the corresponding predefined command language script (see **Steele et al.**, col. 7, lines 33-56), without the necessity to first translate the request into a valid SQL command and then submit the SQL command to the database (as is the case in **Garrison**, col. 8, lines 9-19).

19. Regarding claim 16, **Garrison** teaches an apparatus as claimed, comprising:

a) means located at a site for permitting a user having a user identifier to interact with a database responsively coupled via a publicly accessible digital data communication network (see col. 4, lines 1-32);

b) means responsively coupled to said permitting means via said publicly accessible digital data communication network for offering data processing services involving access to said database in response to said service request (see col. 6, line 60 through col. 7, line 32; see also col. 7, line 50 through col. 8, line 37); and

c) means responsively coupled to said offering means for preventing said offering means from offering said data processing services to said user in response to said service request unless said site corresponds to a security profile wherein said security profile permits access to said database (see col. 6, line 60 through col. 7, line 32; see also col. 7, line 50 through col. 8, line 37), wherein the existence of the security profile renders the claimed administration module inherent, since the only claimed functionality if the administration module is to maintain the security profile, and the reference teaches the maintenance of a security profile at col. 7, lines 50-67 and col. 10, lines 5-17.

Garrison does not explicitly teach an apparatus wherein the user accesses the database without transfer of said user identifier via said publicly accessible digital data communication network.

De Capitani di Vimercati et al., however, teaches an apparatus wherein the user accesses the database without transfer of said user identifier via said publicly accessible digital data communication network (see page 88, col. 2, last paragraph; see also Table 1; see also section 3.2 Authentication, beginning on page 94, all of which teach a mechanism whereby all users accessing a database from a particular site are granted access).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the references, since they are all concerned with the same field of endeavor, that is, remotely accessing databases (see **Garrison**, Abstract; see also **De Capitani di Vimercati et al.**, Abstract).

It would have been furthermore obvious to one of ordinary skill in the art at the time of the invention to provide an authentication mechanism whereby the user identifier need not be transmitted via a publicly accessible digital communication network (i.e., global authentication), since the alternative would be to impose local authentication, wherein users are required to re-authenticate themselves at each local site, which may make the access control process very heavy (see **De Capitani di Vimercati et al.**, page 87, col. 2, last paragraph through page 88, col. 1, first paragraph).

Neither **Garrison** nor **De Capitani di Vimercati et al.** explicitly teaches an apparatus wherein said service request is honored by executing a sequence of command language scripts having an associated security profile.

Steele et al., however, teaches an apparatus wherein a service request is honored by executing a sequence of command language scripts having an associated security profile (see col. 4, line 57 through col. 5, line 4; see also col. 7, lines 33-56).

It would have been obvious to one of ordinary skill in the art at the time of the invention to satisfy service requests through the execution of command language scripts having an associated security profile, since upon receipt of the service request the request can be satisfied merely by executing the corresponding predefined command language script (see **Steele et al.**, col. 7, lines 33-56), without the necessity to first translate the request into a valid SQL command and then submit the SQL command to the database (as is the case in **Garrison**, col. 8, lines 9-19).

20. Regarding claim 2, **Garrison** additionally teaches a data processing environment wherein a security profile is generated by said data management system (see col. 6, line 60 through col. 7, line 32; see also col. 7, line 50 through col. 8, line 37, and particularly security data table 57, storing information defining what data is accessible to which users, the existence of which renders its generation inherent).

21. Regarding claims 3, 8, 12, 13 and 18, **Garrison** additionally teaches an improvement, method and apparatus further comprising a portion of a service request whereby said database management system receives an identifier corresponding to said particular site (see discussion of predefined password at col. 6, line 60 through col. 7, line 32; see also col. 7, line 50 through col. 8, line 37).

22. Regarding claims 4, 14 and 17, **Garrison** additionally teaches an improvement, method and apparatus wherein said publicly accessible digital data communication network further comprises the Internet (see col. 4, lines 1-32).

23. Regarding claim 7, **Garrison** additionally teaches an apparatus wherein said terminal accesses said data entity by transferring a service request to said system (see col. 6, line 60 through col. 7, line 32; see also col. 7, line 50 through col. 8, line 37).

24. Claims 5, 9, 10, 15, 19 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Garrison** (U.S. Patent 6,275,939) in view of **De Capitani di Vimercati et al.** ("Access Control in Federated Systems") in view of **Steele et al.** (U.S. Patent 6,282,175) as applied to claims 1-4, 6-8, 11-

14 and 16-18 above, and further in view of **Unisys** ("UNISYS CSG MarketPlace – The Mapper System").

25. Regarding claims 5 and 19, **Garrison, De Capitani di Vimercati et al.** and **Steele et al.** teach an improvement to a data processing environment, method and apparatus substantially as claimed.

None of **Garrison, De Capitani di Vimercati et al.** nor **Steele et al.** explicitly teaches the improvement, method and apparatus wherein said database management system is a legacy database management system.

However, **Unisys** teaches the database management system MAPPER, constituting a legacy database management system (see entire document).

It would have been obvious to one of ordinary skill in the art at the time of the invention to use MAPPER as the database management system, since MAPPER contains many key features that make its use advantageous for users (see **Unisys**, key features under MAPPER Overview, page 3).

26. Regarding claims 9 and 15, **Garrison, De Capitani di Vimercati et al.** and **Steele et al.** teach an improvement to a data processing environment, method and apparatus substantially as claimed.

None of **Garrison, De Capitani di Vimercati et al.** nor **Steele et al.** explicitly teaches the improvement, method and apparatus wherein said database management system is MAPPER.

However, **Unisys** teaches the database management system MAPPER (see entire document).

It would have been obvious to one of ordinary skill in the art at the time of the invention to use MAPPER as the database management system, since MAPPER contains many key features that make its use advantageous for users (see **Unisys**, key features under MAPPER Overview, page 3).

27. Regarding claim 10, **Garrison** additionally teaches an apparatus wherein said publicly accessible digital data communication network further comprises the World Wide Web (see col. 4, lines 1-32).

28. Regarding claim 20, **Garrison** additionally teaches an apparatus wherein said permitting means further comprises an industry standard personal computer (see col. 4, lines 1-60).

29. Claims 5, 9, 10, 15, 19 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Garrison** (U.S. Patent 6,275,939) in view of **De Capitani di Vimercati et al.** ("Access Control in Federated Systems") in view of **Steele et al.** (U.S. Patent 6,282,175) as applied to claims 1-4, 6-8, 11-14 and 16-18 above, and further in view of **Unisys** ("Why Do I Need Cool ICE?").

30. Regarding claims 5 and 19, **Garrison, De Capitani di Vimercati et al.** and **Steele et al.** teach an improvement to a data processing environment, method and apparatus substantially as claimed.

None of **Garrison, De Capitani di Vimercati et al.** nor **Steele et al.** explicitly teaches the improvement, method and apparatus wherein said database management system is a legacy database management system.

However, **Unisys** teaches a system wherein the database management system used is MAPPER, constituting a legacy database management system (see page 3, second paragraph).

It would have been obvious to one of ordinary skill in the art at the time of the invention to use MAPPER as the database management system, since MAPPER has been tuned for reliability, scalability, and high performance, and furthermore, since the technology has been used for years by thousands of users for many different kinds of applications, and since it has gained a reputation for performing well for everything from small data analysis applications to huge transaction systems, and since its reliability is exemplary (see **Unisys**, page 3, second paragraph).

31. Regarding claims 9 and 15, **Garrison, De Capitani di Vimercati et al.** and **Steele et al.** teach an improvement to a data processing environment, method and apparatus substantially as claimed.

None of **Garrison, De Capitani di Vimercati et al.** nor **Steele et al.** explicitly teaches the improvement, method and apparatus wherein said database management system is MAPPER.

However, **Unisys** teaches a system wherein the database management system used is MAPPER (see page 3, second paragraph).

It would have been obvious to one of ordinary skill in the art at the time of the invention to use MAPPER as the database management system, since MAPPER has been tuned for reliability, scalability, and high performance, and furthermore, since the technology has been used for years by thousands of users for many different kinds of applications, and since it has gained a reputation for performing well for everything from small data analysis applications to huge transaction systems, and since its reliability is exemplary (see **Unisys**, page 3, second paragraph).

32. Regarding claim 10, **Garrison** additionally teaches an apparatus wherein said publicly accessible digital data communication network further comprises the World Wide Web (see col. 4, lines 1-32).

33. Regarding claim 20, **Garrison** additionally teaches an apparatus wherein said permitting means further comprises an industry standard personal computer (see col. 4, lines 1-60).

Response to Arguments

34. Applicant's arguments filed 30 December 2004 have been fully considered but they are not persuasive.

35. Regarding the Applicants' argument that the examiner's rejection of claims 1-20 under 35 U.S.C. § 112, first paragraph should be withdrawn, in view of the Applicants' arguments and amendment to the specification, the examiner finds these arguments persuasive. The Applicants' comments regarding the fact that the disclosures of Figures 13 and 14 are enabling to an ordinary artisan in the field of computer programming with the use of the commercially available Cool ICE product are particularly well taken.

36. Regarding the Applicants' argument that there would be no motivation to combine the **Garrison** reference with that of **De Capitani di Vinercati** because the latter reference teaches away from such a combination, the examiner respectfully disagrees.

The portion of the **De Capitani di Vinercati** reference cited in support of the Applicants' argument says that other approaches are preferable *in general*, which does not preclude situations wherein the approach would in fact be the preferred approach. In fact, the reference teaches that providing an authentication mechanism whereby the user identifier need not be transmitted via a publicly accessible digital communication network (i.e., global authentication) is desirable, since the alternative would be to impose local authentication, wherein users are required to re-authenticate themselves at each local site, which may make the access control process very heavy (see **De Capitani di Vimercati et al.**, page 87, col. 2, last paragraph through page 88, col. 1, first paragraph).

37. Regarding the Applicants' argument that the examiner has not provided any information regarding the likelihood of success for any of the combination of references, the examiner respectfully responds that in the field of computer programming, success is assured in the incorporation of a feature into a piece of software. Unlike the chemical or mechanical arts where a given combination of chemicals or design of a part may not achieve the desired results, given a competent software engineer and programmer, any desired functionality can be implemented in any given software application.

Thus, an ordinary artisan can reasonably be expected to successfully incorporate a feature from one software product into another software product.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Luke S. Wassum whose telephone number is 571-272-4119. The examiner can normally be reached on Monday-Friday 8:30-5:30, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John E. Breene can be reached on 571-272-4107. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

In addition, INFORMAL or DRAFT communications may be faxed directly to the examiner at 571-273-4119.

Customer Service for Tech Center 2100 can be reached during regular business hours at (571) 272-2100, or fax (703) 872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Luke S. Wassum
Primary Examiner
Art Unit 2167

lsw
28 April 2005